

Sicurezza e privacy I

Introduzione al corso

Logistica

- ◆ Docente:
 - ◆ Piero Bonatti
 - ◆ Studio 0F-34 nell'edificio di Biologia
 - ◆ bonatti@na.infn.it
- ◆ Pagina del corso
 - ◆ Home di Piero Bonatti => Teaching
 - ◆ <http://people.na.infn.it/~bonatti/didattica/>
- ◆ Ricevimento:
 - ◆ Per appuntamento (e-mail)

Materiale didattico

- ◆ Stallings: Sicurezza delle reti. Mc Graw Hill
- ◆ Note del docente su linguaggi logici
- ◆ Articoli di supporto per la prima parte del corso
 - ◆ Terminologia e concetti di base
 - ◆ Modelli di politiche
 - ◆ Meccanismi
- ◆ Slides
 - ◆ Tutto reperibile sul sito del corso a parte il libro
 - ◆ [secpriv](#)
 - ◆ [pgpp3p](#)

Contenuti

- ◆ Panoramica su sicurezza e privacy
 - ◆ Problematiche
 - ◆ Cenni alle soluzioni
 - ◆ Con approfondimenti su alcuni argomenti
- ◆ Insegnamento molto interdisciplinare e “trasversale”
 - ◆ Teoria, tecnologie, applicazioni

Sicurezza è

- ◆ Protezione delle informazioni digitali mediante crittografia
 - ◆ Tecniche algebriche; complessità computazionale
- ◆ Protezione dallo sfruttamento di banchi
 - ◆ Nei S.O. e nei protocolli di rete
 - ◆ Nelle applicazioni
 - ◆ *Best practice* e standards per gestione emergenze (tecniche di software engineering)
- ◆ Configurazione politiche nel rispetto di vincoli di comportamento
 - ◆ Modelli logici e statistici
 - ◆ Tecniche di ottimizzazione combinatoria e A.I.

Sicurezza è anche

- ◆ Applicazione delle tecniche crittografiche per ottenere primitive di più alto livello
 - ◆ Posta elettronica sicura, votazioni, ...
 - ◆ Tecniche algoritmiche
- ◆ Affidabilità, software sicuro
 - ◆ Tecniche di analisi e verifica formali del software
 - ◆ Trattati dai Proff. Benerecetti e Peron nei corsi di specifica e verifica formale del software

Distribuzione nei semestri

- ◆ Primo semestre
 - ◆ 2 ore/settimana
 - ◆ Concetti di base
 - ◆ Modelli di politiche
 - ◆ Linguaggi per la specifica di politiche
 - ◆ Meccanismi
- ◆ Secondo semestre
 - ◆ 4 ore/settimana
 - ◆ Network security
 - ◆ Crittografia
 - ◆ Aspetti avanzati
 - ◆ Privacy

Esami

- ◆ Scritto + orale
 - ◆ Esempi sul sito del corso
 - ◆ Esercitazioni verso la fine del corso
- ◆ In caso di scritti disastrosi non è possibile ritentare l'esame nella stessa sessione
 - ◆ Se non si consegna è come non avere partecipato
- ◆ È... matematico che vengano chieste le dimostrazioni dei (pochi) teoremi presentati nel corso

Fine introduzione

Domande?